

Appl. No. 10/065,291  
Amdt. dated July 07, 2006  
Reply to Office action of April 07, 2006

**Amendments to the Claims:**

This listing of claims will replace all prior versions and listings of claims in the application:

**Listing of Claims:**

- 1 (currently amended): A method for applying for crypto-keys from a network system, the network system comprising at least a first user client, an access point having an identifying module and a user list, and a certificate server, the access point being used to receive a certificate packet from the first user client and to utilize the identifying module to verify the certificate packet according to the user list so as to generate a verification signal, the certificate server being used to generate a pair of distinct crypto-keys according to the verification signal and a first algorithm, the method comprising:
- utilizing the first user client to ~~generating~~ generate the certificate packet;
  - utilizing the access point to receive the certificate packet;
  - utilizing the identifying module to verify the certificate packet according to the user list so as to generate the verification signal, and transmitting the verification signal to the certificate server;
  - utilizing the certificate server to generate the pair of distinct crypto-keys according to the first algorithm;
  - controlling the certificate server to transmit the pair of crypto-keys to the access point; and
  - controlling the access point to transmit the pair of crypto-keys to the first client.
- 2 (original): The method of claim 1 wherein the certificate packet comprises a user name and a password.
- 3 (currently amended): The method of claim 1 wherein the first algorithm is a Rivest

BEST AVAILABLE COPY

Appl. No. 10/065,291  
Amdt. dated July 07, 2006  
Reply to Office action of April 07, 2006

Shamir ~~Asleman~~ Adelman (RSA) algorithm.

4 (original): The method of claim 1 wherein the first algorithm is a digital signature algorithm (DSA).

5 (original): The method of claim 1 wherein the pair of crypto-keys is a public key and a private key.

6 (original): The method of claim 1 wherein the network system further comprises at least a second user client communicating with the access point, and the first user client comprises a first encryption module for encrypting a plain text into a ciphered text according to a second algorithm and a first key of the pair of crypto-keys, the second user client comprises a second decryption module for decrypting the ciphered text into the plain text according to a third algorithm and a second key of the pair of crypto-keys, the method further comprising:

transmitting the second key from the first user client through the access point to the second user client;

utilizing the first encryption module to encrypt the plain text into the cipher text according to the second algorithm and the first key;

transmitting the ciphered text from the first user client through the access point to the second user client; and

utilizing the second decryption module to decrypt the ciphered text according to the third algorithm and the second key.

7 (original): The method of claim 6 wherein the second algorithm and third algorithm are associated with the first algorithm.

8 (original): The method of claim 6 wherein the first user client further comprises a first

## BEST AVAILABLE COPY

Appl. No. 10/065,291  
Amdt. dated July 07, 2006  
Reply to Office action of April 07, 2006

decryption module for decrypting the ciphered text into the plain text according to the third algorithm and the first key, and the second user client further comprises a second encryption module for encrypting the plain text into the ciphered text according to the second algorithm and the second key, the method further comprising:

- utilizing the second encryption module to encrypt the plain text into the ciphered text according to the second algorithm and the second key;
- transmitting the plain text from the second user client through the access point to the first user client; and
- utilizing the first decryption module to decrypt the ciphered text according to the third algorithm and the first key.

9 (original): The method of claim 1 wherein the network system further comprises at least a second user client communicating with the access point, and the first user client comprises a first encryption module for encrypting numbers according to a second algorithm and a first key of the pair of crypto-keys, the second user client comprises a second decryption module for decrypting numbers according to a third algorithm and a second key of the pair of crypto-keys, the method further comprising:

- transmitting the second key from the first user client through the access point to the second user client;
- controlling the first user client to convert a plain text into a first value according to a fourth algorithm;
- utilizing the first encryption module to encrypt the first value according to the second algorithm and the first key;
- transmitting the plain text and the encrypted first value from the first user client through the access point to the second user client;
- utilizing the second decryption module to decrypt the encrypted first value according to the third algorithm and the second key;

**BEST AVAILABLE COPY**

Appl. No. 10/065,291  
Amdt. dated July 07, 2006  
Reply to Office action of April 07, 2006

controlling the second user client to convert the plain text into a second value according to the fourth algorithm; and  
comparing the second value with the decrypted first value to verify the plain text transmitted from the first user client to the second user client.

10 (original): The method of claim 9 wherein the fourth algorithm is a message digest 2 (MD2) algorithm.

11 (original): The method of claim 9 wherein the fourth algorithm is a message digest 5 (MD5) algorithm.

12 (original): The method of claim 9 wherein the fourth algorithm is a secure Hash algorithm (SHA).

13 (original): The method of claim 9 wherein the second algorithm and third algorithm are associated with the first algorithm.

14 (currently amended): The method of claim 9 wherein the first user client further comprises a first decryption module for decrypting numbers according to the third algorithm and the first key, and the second user client further comprises a second encryption module for encrypting numbers according to the second algorithm and the second key, the method further comprising:

controlling the second user client to convert the plain text to the first value according to the fourth algorithm;  
utilizing the second encryption module to encrypt the first value according to the second algorithm and the second key;  
transmitting the plain text and the encrypted first value from the second user client through the access point to the first user client;

## BEST AVAILABLE COPY

Appl. No. 10/065,291  
Amdt. dated July 07, 2006  
Reply to Office action of April 07, 2006

utilizing the first decryption module to decrypt the encrypted first value according to the third algorithm and the first key;  
controlling the first user client to convert the plain text to the second value according to the fourth ~~forth~~ algorithm; and  
comparing the second value with the decrypted first value to verify the plain text transmitted from the second user client to the first user client.